Exam : NSE7_OTS-7.2

Title : Fortinet NSE 7 - OT Security7.2

https://www.passcert.com/NSE7_OTS-7.2.html

1.An OT network administrator is trying to implement active authentication.
Which two methods should the administrator use to achieve this? (Choose two.)
A. Two-factor authentication on FortiAuthenticator
B. Role-based authentication on FortiNAC
C. FSSO authentication on FortiGate
D. Local authentication on FortiGate
Answer: A,D

2.An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM.
Which step must the administrator take to achieve this task?
A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
B. Create a notification policy and define a script/remediation on FortiSIEM.
C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.
Answer: B
Explanation:
Reference:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/06918379-afd1-11e9-a989-00505692583a/Standalone_PDF.pdf

3.An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.
What should the OT supervisor do to achieve this on FortiGate?
A. Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
B. Enable two-factor authentication with FSSO.
C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
D. Under config user settings configure set auth-on-demand implicit.
Answer: D

4.Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)
A. FortiNAC
B. FortiManager
C. FortiAnalyzer
D. FortiSIEM
E. FortiGate
Answer: A,D,E

5.Refer to the exhibit.

```
config system interface
     edit VLAN101_dmz
          set forward-domain 101
next
     edit VLAN101_internal
          set forward-domain 101
end
```

Given the configurations on the FortiGate, which statement is true?

A. FortiGate is configured with forward-domains to reduce unnecessary traffic.

B. FortiGate is configured with forward-domains to forward only domain controller traffic.

C. FortiGate is configured with forward-domains to forward only company domain website traffic.

D. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

Answer: A

6.An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device.

Which statement about the industrial signature database on FortiGate is true?

A. A supervisor must purchase an industrial signature database and import it to the FortiGate.

B. An administrator must create their own database using custom signatures.

C. By default, the industrial database is enabled.

D. A supervisor can enable it through the FortiGate CLI.

Answer: D